

# Evidence shows Syrian security got comms from West

July 16 2012, by RAPHAEL SATTER

---



The offices of Intracom are seen in this photo taken Athens on Tuesday July 10, 2012. Leaked company emails and senior employees say that two European contractors were putting the finishing touches on Syria's encrypted radio system as the revolt against Damascus got under way last year. Documents made available to The Associated Press and other media organizations by the WikiLeaks organization show that Greece's Intracom S.A. and Italy's Selex Elsag, a unit of Finmeccanica S.p.A., spent years building a Syria-wide communications network and equipped the government with thousands of walkie-talkies, motorcycle-mounted radio units and avionic transceivers used in helicopters. Both companies say they've complied with sanctions rules, and experts say the transfers were likely to have been legal. (AP Photo/Petros Giannakouris)

(AP) — As violence began racing through Syria last year, two European contractors were putting the finishing touches on an encrypted radio system that Syrian officials intended for their security forces, according

to leaked company emails and three senior employees involved in the project.

The documents — made available to The Associated Press and other media organizations by the WikiLeaks organization — show that Greece's Intracom S.A. and Italy's Selex Elsag spent years building a [Syria](#)-wide communications network and equipped the government with thousands of walkie-talkies, motorcycle-mounted radio units and avionic transceivers used in helicopters.

The leaked documents give an unusually detailed look at the communications help Western companies have been providing Syria's regime — something activists find disturbing.

"This kind of technological assistance is highly undesirable because it is used to repress people," said European parliamentarian Marietje Schaake, who has pushed for tighter export controls on authoritarian governments. "The fact that these are EU-based companies doing all this hurts our credibility."

Most sanctions-watchers interviewed by the AP say that Selex and Intracom likely acted lawfully, and the companies themselves denied wrongdoing.

Intracom said in a statement that it had supplied the Syrians with a civilian telecommunications system "in full respect of relevant export regulations," adding that it was no longer involved in operating the system and therefore had no control over how it was used. It said that its work in Syria had since been suspended due to the situation there.

Selex owner Finmeccanica S.p.A. echoed Intracom's statement, saying its communications system was intended "exclusively for civil, and not military use." The Rome-based defense contractor also claimed that the

project was completed "prior to the outbreak of the country's internal conflicts."

Both statements seemed hard to square with evidence that elements of the communication system were designed with the military in mind, or emails showing that Selex and Intracom had been providing technical support to Syrian officials as recently as February — a time when government forces were using artillery to pound rebel-held areas of the Syrian city of Homs.

Intracom spokesman Alexandros Tarnaris refused to answer a series of detailed questions about the apparent discrepancies between his company's statement and the evidence seen by the AP; Selex spokesman Carlo Maria Fenu also declined to answer questions.

---

The companies' role in Syria is difficult to disentangle. In 2008 they jointly announced a €40 million deal to build a mobile radio system for the Syrian Wireless Organization, an arm of Syria's Ministry of Communication and Technology. Selex supplied the radio terminals; Intracom built much of the network's infrastructure.

The type of system they were building is called a terrestrial trunked radio, or TETRA, a technology employed the world over to provide resilient, long-range communication for emergency workers, transport services and private industry. In Britain, it's used everywhere from the country's coast guard agency to London's Heathrow Airport and the capital's sprawling subway.

But the technology — considered more secure than conventional cell phone networks — has law enforcement and military applications as well. Police agencies across Europe use the standard to communicate,

while Israel uses a Motorola-built TETRA network for its army.

"Like any technologies it can be used for good or evil," said Marcus Carey, a researcher with Boston-based security company Rapid7. "While an emergency organization can save lives with . TETRA networks, an oppressive regime can coordinate violent actions against dissidents."

The leaked documents provide a partial picture of how the companies saw TETRA being used in Syria, but they make clear that a large chunk of their equipment was earmarked for the country's police force — much of it shipped even as revolt against Damascus was gathering steam.

"This is going to Muadamia Police warehouse," says an Intracom email dated May 7, 2011 — the same month that New York-based Human Rights Watch warned that officers were subjecting political opponents to a campaign of arbitrary arrests, intimidation, and torture.

The email, which refers obliquely to the "current situation," itemizes what appear to be several hundred radios destined for the Damascus suburb. Among them are shock-resistant Selex VS3000s, which a company brochure advertises as being "compliant with most military-standard environmental conditions."

Although there's ample evidence that Intracom knew much of the companies' material was destined for the [security](#) forces, the AP has not seen any direct evidence that Selex knew where its equipment was going.

Itemized bills give a feel for the scope of the construction work involved in building the TETRA network — although crucial details such as timing are hard to work out.

One bill sent by an Intracom employee and dated May 10, 2011, lists more than €100,000 worth of equipment installed at two separate

Damascus police sites, including antennae, microwave radio equipment and air-conditioning systems.

Another itemized list — this one attached to an Intracom email sent Feb. 2, 2012 — notes €300,000 worth of costs associated with a Police Administration Center in the Syrian city of Aleppo, as well as references to work carried out at a police academy in Damascus, two further traffic police sites in the capital and a fourth police site in the Damascus suburb of Barzeh.

Also in that sloppily-spelled list — and highlighted in red — is a Damascus-based site labeled "Military."

—

That note was one of a handful of references to the military in the leaked documents. One senior manager who worked with Intracom to set up the network said that the army's needs played a major role in the project.

"It's used by the military," he told AP, adding that many of the project's mobile radio terminals were intended for installation in army vehicles.

He spoke on condition of anonymity, saying he didn't want to draw attention to himself.

The notion of an army link to Intracom's work is backed by the leaked emails.

A May 19, 2011, email to Intracom employees from a subcontractor refers to the drafting of a "report for the Installation of the radio Terminal in military Car." A July 2011 survey document notes the contact details for a radio repeater simply as: "Army." In another email, sent in March 2011, Intracom employee Ghassan Nakoul tells co-

workers that "we are going to connect the network with military exchange."

Nakoul, who spoke briefly when reached by phone, confirmed having been told "one or two times" by the Syrian Wireless Organization that Intracom was doing work for the military but said he had "honestly no idea" for whom the TETRA network was really meant.

Nakoul suggested that officials at the organization may have been exaggerating the seriousness of the project in order to get it finished more quickly.

"They sometimes raise (their) importance," he said. "Sometimes they say 'this is (for) police,' 'this is (for) the military.'"

One Intracom employee, who spoke on condition of anonymity because he did not want to make his role in the project known, confirmed the broad outlines of the work in Syria, acknowledging that it had a "public safety" aspect.

It's not clear what role, if any, Selex played in discussions over the technology's military applications.

The nature of the Syrian Wireless Organization — whose website couldn't be located — is obscure. Emails sent to Maamoun Haj Ibrahim and Riad Naouf — men listed by the U.N. as directors of the organization — were not returned. Calls to the group rang unanswered for days.

Syrian Foreign Ministry spokesman Jihad Makdissi said he didn't know anything about the matter and didn't respond to an email requesting comment from someone who did.

---

Building a nationwide TETRA network was a major undertaking.

Intracom manager Mohammad Shoorbajee's profile on the professional-networking site LinkedIn — which he has since modified to remove all reference to his work — said the project included the construction of 130 base stations, four command-and-control centers, dispatch stations, core switches, and the delivery of some 17,000 Selex radios across Syria.

A billing document dated Oct. 19, 2011, broke the equipment down, listing more than 11,000 walkie-talkies, 3,500 mobile radio units for use in vehicles, 1,600 radio dispatch consoles, 1,400 motorcycle-mounted units, 60 marine units for use on sea, and 30 avionic transceivers for use in helicopters.

Several lawyers and activists said the shipments likely weren't in breach of EU sanctions, first imposed on Syria back in May of 2011 and repeatedly strengthened since.

Zia Ullah, a London-based attorney with Pannone LLP, said he believed the shipments were on the right side of the law, adding that conflicts like the one in Syria put economy-conscious Europeans in a tricky spot.

"To the extent that equipment is being used or supplied to the Syrian regime, is that politically what the EU wants to see?" he said. "On the other hand, for many of these companies, it's a lifeline commercially, particularly in countries like Greece and Italy."

But Matthew Parish, a Geneva-based attorney with U.K. law firm Holman Fenwick Willan LLP, said that the vagueness of EU sanctions law meant that the situation was "very arguable either way."

"Given the ambiguity of the language in the EU decisions, I think what you can say that what they did in the past is borderline," he said.

Borderline cases have received an increasing amount of attention as pro-democracy uprisings in the Arab world have torn the lid off the machinery of state surveillance. Last year The Wall Street Journal revealed that Syrian officials were using Internet filtering devices made by California's Blue Coat Systems Inc. In November Bloomberg reported that Italian company Area S.p.A. had been using U.S. technology to equip Damascus with a powerful mass surveillance network. Blue Coat has said it didn't know its technology was bound for Syria; Area has said it's considering how to pull out of its contract.

Schaake, the parliamentarian, said she thought those companies were just the tip of the iceberg.

"There are far more companies whose name we don't know," she said.

---

Intracom and Selex's work in Syria has continued until recently. On Dec. 29, 2011, Intracom's Ilias Moschonas wrote to his team to say that there were still problems with the TETRA network and that engineers might be needed to provide on-the-job training in basic repairs and other skills in Damascus early in the new year.

Around the same time, Intracom's Nakoul described a trip to provide tech support at a petroleum facility near the Syrian city of Deir el-Zour, a trip he did not seem eager to repeat.

"Deir alzor is not calm city (armed people everywhere) and my opinion is to have a clear solution for this case before we go over there again," he warned his colleagues.



On Feb. 2, 2012, Moschonas wrote again to inform his colleagues that Selex engineers would be in Damascus that month to deliver equipment needed to fix Syria's helicopter transceivers and train local employees on how to make repairs.

The leaked emails don't go further than March 2012, so it's not clear whether the engineers ever made it to the Syrian capital.

It's also unclear whether Intracom or Selex's work in the country continued beyond that date, although draft warranty documents circulated by Shoorbajee and others envisioned both companies acting in tandem to provide tech support, software updates, and repairs.

Moschonas did not return emails seeking comment and neither Intracom nor Selex have said whether they were still replacing damaged parts, uploading new software, or helping fix faulty equipment.

Nakoul denied that he or his company had taken sides in the conflict gripping Syria, saying that he'd already received death threats from rebel sympathizers after WikiLeaks published his email address.

"We are just technical people," he said. "We are just working on a project.

"We are not on any side."

**More information:** Online:

WikiLeaks: [wikileaks.org](http://wikileaks.org)

Intracom: [www.intracom.gr](http://www.intracom.gr)

Finmeccanica: [www.finmeccanica.it](http://www.finmeccanica.it)

Copyright 2012 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: Evidence shows Syrian security got comms from West (2012, July 16) retrieved 19 April 2024 from <https://phys.org/news/2012-07-evidence-syrian-comms-west.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.